Claims

1.   In an electronic device, a method, comprising the steps of:

providing a user profile holding information regarding a user;

5   establishing a first set of permissions for the user profile, wherein said first set of permissions specifies who may access the user profile;

establishing a second set of permissions for a selected sub-division of the user profile, wherein said second set of permissions specifies who may access the sub-division; and

10   wherein in order for a party to access the selected sub-division, the party must be specified by the first set of permissions as having access to the user profile and must be specified by the second set of permissions as having access to the selected sub-division.

15   2.   The method of claim 1, wherein the sub-division is a field.

3.   The method of claim 1, wherein the first set of permissions specifies what type of access to the user profile is granted to those who may access the user profile.

20   4.   The method of claim 4, wherein at least one party is granted read access to the user profile, indicating that the party may read information in the user profile.

5.   The method of claim 4, wherein at least one party is granted write access to the user profile, indicating that the party may write information into the user profile.

25

6.   The method of claim 4, wherein at least one party is granted availability access to the user profile, indicating that the party may find out whether the user profile is available.

30   7.   The method of claim 4, wherein at least one party is granted delete access to the user profile, indicating that the user may delete information in the user profile.

8.   The method of claim 1, wherein the second set of permissions specifies who may access the user profile.

35

9.   The method of claim 1, wherein one of the first set of permissions and the second set of permissions contains a list of parties that may access the user profile and the sub-division, respectively.

5   10.   The method of claim 1, wherein defined groups of parties are provided and wherein at least one of the first set of permissions and the second set of permissions specifies one of the groups as having access.

11.   The method of claim 1, wherein the user specifies at least one of the first set of
10   permissions and the second set of permissions.

12.   The method of claim 1, wherein at least one of the first set of permissions and the second set of permissions is established by default.

15   13.   The method of claim 1, further comprising the step of establishing a third set of permissions for an additional one of the sub-divisions in the user profile, wherein said third set of permissions specifies who may access the additional sub-division.

14.   The method of claim 12, wherein the sub-division of the user profile are
20   organized hierarchically and wherein the sub-division contains the additional sub-division.

15.   The method of claim 1, wherein defined groups are provided and wherein at least one of the first set of permissions and the second set of permissions specifies who may
25   have access as an access set, said access set resulting from a set algebraic operation performed on at least two of the groups.

16.   A method, comprising the steps of:
            providing user profiles that hold information regarding users and are
30   accessible via a network;
            specifying groups of service providers for providing services to the users, each group containing a set of service providers; and
            granting access permission for authorized information in a selected user profile to a selected one of the groups so that the service providers in the selected
35   group may access the authorized information.

17.   The method of claim 16, wherein the service providers in the selected group all provide a common category of service.

18.   The method of claim 16, wherein at least one group contains other groups that
5   constitute subsets of the group, and said groups containing logically related service providers.

19.   The method of claim 16, wherein the user profiles are accessible via a centralized repository and wherein the authorized information in the user profile may be
10   accessed by service providers that did not directly solicit the accessible information from the user.

20.   In an electronic device, a method, comprising the steps of:
            providing a user profile having various fields, wherein at least one of said
15   fields has associated permissions;
            setting the permissions relative to a given service provider so as to
        prevent access to at least one selected field and grant access to at least one given
        field in the user profile so as to support an anonymous transaction between the
        given service provider and the user by withholding an identity of the user.
20
21.   The method of claim 20, wherein the user profile contains a name field holding a name of the user and wherein the selected field is the name field.

22.   The method of claim 20, wherein the user profile contains an address field
25   holding an address field holding an address of the user and wherein the selected field is the address field.

23.   The method of claim 20, wherein the permissions are set to block access to multiple ones of the fields by the given service provider.
30
24.   The method of claim 20, wherein the user profile contains a payment field holding information regarding a payment mechanism and wherein the given field is the payment field.

35   25.   The method of claim 20, wherein the user profile contains a credit card field holding credit card number and wherein the select field is a credit card field.

26.   In an electronic device, a method, comprising the steps of:

providing a user profile holding information regarding a user in fields;

providing a protocol that enables the getting and setting of the following:

(i)   fields in the user profile;

(ii)   access permissions for the fields in the user profile;

(iii)   members of groups that have access permissions to selected ones of the fields in the user profile;

(iv)   group access permissions that specify access information regarding groups;

(v)   permissions access permissions that specify permissions for the access permissions; and

(vi)   a schema definition for the user profile.